AMENDMENT OF THE CLAIMS

1. (Original) A system for performing cryptographic operations on network data, the system comprising:

an input interface configured to receive data into the system;

a plurality of processors in a cascaded arrangement, each processor having an input coupled to the input interface and an output coupled to respective inputs of each of the other processors downstream in the arrangement, the processors each configured to perform respective cryptographic operations on the data; and

an output interface coupled to the input interface and to the output of each of the processors, the output interface configured to transmit data out of the system and to direct the data through the system in coordination with the input interface according to a predetermined algorithm.

2. (Original) The system of claim 1, wherein the plurality of processors comprises:

a first processor having its data inputs coupled only to the input interface, the first processor configured to compress uncompressed data and to decompress compressed data.

3. (Original) The system of claim 2, wherein the first processor is configured to compress and decompress the data according to at least one of a Lempel-Ziv-Stac (LZS) and an Adaptive Lossless Data Compression (ALDC) compression algorithm.

4. (Original) The system of claim 2, wherein the plurality of processors comprises:

a second processor having a first input coupled to the input interface and a second input coupled to an output of the first processor, the second processor configured to obscure non-secure data and to decipher secure data.

5. (Original) The system of claim 4, wherein the second processor is configured to obscure and decipher the data according to at least one of a Data Encryption Standard (DES), a Triple-DES, and an Advanced Encryption Standard (AES) algorithm.

6. (Original) The system of claim 4, wherein the plurality of processors comprises:
a third processor having a first input coupled to the input interface, a second input coupled to an output of the first processor, and a third input coupled to an output of the second processor, the third processor configured to determine an integrity of the data.

7. (Original) The system of claim 6, wherein the third processor is configured to determine the integrity by hashing the data according to at least one of a Secure Hash Algorithm (SHA-1) and a Message Data 5 (MD5) algorithm.

8. (Original) The system of claim 1, wherein the predetermined algorithm is based on control information included in a security association related to the data.

9. (Original) The system of claim 8, wherein the input interface is configured to receive the control information and to forward the control information to each of the processors for use in performing the respective cryptographic operations on the data.

10. (Original) The system of claim 9, wherein the control information includes at least one of:
an identity of an authentication algorithm used to hash the data;
an identity of an encryption algorithm used to obscure and decipher the data;
keying material used by at least one of the authentication and encryption algorithms; and
a lifetime of the security association related to the data.

11. (Original) The system of claim 1, comprising:

logic configured to determine a checksum associated with the data transmitted out of the system.

12. (Original) A method for performing cryptographic operations on network data, the method comprising:

receiving data;

directing the received data through a cascaded arrangement of processors according to a predetermined algorithm, each processor having an input coupled to the received data and an output coupled to respective inputs of each of the other processors downstream in the arrangement;

performing respective cryptographic operations defined by the predetermined algorithm on the received data using the plurality of processors; and

transmitting the operated-on data after performing the cryptographic operations defined by the predetermined algorithm.

13. (Original) The method of claim 12, comprising:

compressing uncompressed received data and decompressing compressed received data using a first processor in the arrangement having its data inputs coupled only to the received data.

14. (Original) The method of claim 13, comprising:

compressing and decompressing the received data according to at least one of a Lempel-Ziv-Stac (LZS) and an Adaptive Lossless Data Compression (ALDC) compression algorithm.

15. (Original) The method of claim 13, comprising:

obscuring non-secure data and deciphering secure data using a second processor in the arrangement having a first input coupled to the received data and a second input coupled to an output of the first processor.

16. (Original) The method of claim 15, comprising:
obscuring and deciphering the data according to at least one of a Data Encryption Standard (DES), a Triple-DES, and an Advanced Encryption Standard (AES) algorithm.

17. (Original) The method of claim 15, comprising:
determining an integrity of the data using a third processor in the arrangement having a first input coupled to the received data, a second input coupled to an output of the first processor, and a third input coupled to an output of the second processor.

18. (Original) The method of claim 17, comprising:
hashing the data to determine the integrity according to at least one of a Secure Hash Algorithm (SHA-1) and a Message Data 5 (MD5) algorithm.

19. (Original) The method of claim 12, comprising:
determining the predetermined algorithm based on control information included in a security association related to the received data.

20. (Original) The method of claim 19, comprising:
receiving the control information; and
forwarding the control information to each of the processors for use in performing the respective cryptographic operations on the data.

21. (Original) The method of claim 20, comprising:
including in the control information at least one of:
an identity of an authentication algorithm used to hash the data;
an identity of an encryption algorithm used to obscure and decipher the data;
keying material used by at least one of the authentication and encryption algorithms; and
a lifetime of the security association related to the data.

22. (Original) The method of claim 12, comprising:
determining a checksum associated with the transmitted data.

23. (Currently Amended) A ~~computer readable medium containing a computer program~~ computer program product comprising a computer useable medium having a computer readable program for performing cryptographic operations on network data, wherein the computer ~~program comprises executable instructions for~~ readable program when executed on a computer causes the computer to perform operations comprising:
receiving data;
directing the received data through a cascaded arrangement of processors according to a predetermined algorithm, each processor having an input coupled to the received data and an output coupled to respective inputs of each of the other processors downstream in the arrangement;
performing respective cryptographic operations defined by the predetermined algorithm on the received data using the plurality of processors; and
transmitting the operated-on data after performing the cryptographic operations defined by the predetermined algorithm.

24. (Currently Amended) The ~~computer readable medium~~computer program product of claim 23, wherein the computer readable program comprises executable instructions for:
compressing uncompressed received data and decompressing compressed received data using a first processor in the arrangement having its data inputs coupled only to the received data;
obscuring non-secure data and deciphering secure data using a second processor in the arrangement having a first input coupled to the received data and a second input coupled to an output of the first processor; and
determining an integrity of the data using a third processor in the arrangement having a first input coupled to the received data, a second input coupled to an output of the first processor, and a third input coupled to an output of the second processor.

25. (Currently Amended) The ~~computer readable medium~~computer program product of claim 24, wherein the computer readable program comprises executable instructions for:

compressing and decompressing the received data according to at least one of a Lempel-Ziv-Stac (LZS) and an Adaptive Lossless Data Compression (ALDC) compression algorithm;

obscuring and deciphering the data according to at least one of a Data Encryption Standard (DES), a Triple-DES, and an Advanced Encryption Standard (AES) algorithm; and

hashing the data to determine the integrity according to at least one of a Secure Hash Algorithm (SHA-1) and a Message Data 5 (MD5) algorithm.

26. (Currently Amended) The ~~computer readable medium~~computer program product of claim 23, wherein the computer readable program comprises executable instructions for:

determining the predetermined algorithm based on control information included in a security association related to the received data;

receiving the control information; and

forwarding the control information to each of the processors for use in performing the respective cryptographic operations on the data.

27. (Currently Amended) The ~~computer readable medium~~computer program product of claim 23, wherein the computer readable program comprises executable instructions for:

determining a checksum associated with the transmitted data.